REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejection of Claims 1, 3-5, and 7 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent No. 5,602,918 (Chen)

This rejection is respectfully traversed on the grounds that neither the Schneier article nor the Chen patent, whether considered individually or in any reasonable combination, discloses or suggests a chipcard **initialization** step in which:

- parts of respective first and second "values" are respectively generated by the card *and* processing station;
- the processing station determines a secret initial value from at least part of the first value and the transmitted part of the second value; and
- the chip card determines the same secret initial value from at least part of the second value and the transmitted part of the first value, ***without the need to actually exchange any part of the secret"initial" value used to initialize the card.***

The Schneier article does not involve any sort of initialization (providing a card with secret keys), while the Chen patent simply discloses "**storage**" of the keys on the card. According to the conventional card initialization procedure, to "**store**" keys on a card, they must be **transferred**, which is contrary to the claimed invention in which the secret keys on the card are generated in parallel with complementary secret keys, *and no part of the keys are exchanged, in either plain text or encrypted form*. There is no suggestion in the Chen patent that the storage of keys on the card involves anything other than the usual transfer.

Instead of the claimed card initialization method, the **Chen** patent appears to disclose an initialization method similar to that of the prior art described on pages 1 and 2 of Applicant's specification, in which at least parts of the data required to initialize the card must be transmitted in **plain text**. Therefore, the Chen patent could not have suggested application of the key

generation method of Schneier to card initialization. The **Schneier** article discloses a data exchange algorithm (the Diffie-Hellman algorithm) that is suitable for exchanging data with an **already initialized** card (*i.e.*, one that already includes encryption keys), but that is not disclosed as being suitable for card initialization requiring data to be written to the card so that Diffie-Hellman exchanges can *subsequently* be carried out, and nothing in the Chen patent suggests otherwise. The Schneier article is not concerned with how the secret values used to generate the session keys were established in the first place (the initialization procedure).

Of the applied references, only the Chen patent even mentions card initialization. However, like the prior art described on pages 1 and 2 of the specification, the Chen patent requires the initialization to be performed at a "***physically secure location***" (col. 4, line 6). This is because, in order to prepare the card to perform DES encryption, the DES key must be transferred to the card. Since the card has not previously been provided with keys, the transfer is carried out by means of plain text. That is the reason that a "physically secure location" is required. **If Chen had found a way to modify the Diffie-Hellman algorithm taught by Schneier so as to enable initialize the card, then a "*physically secure location*" would not have been required.**

The prior art may be summarized as follows:

a. The Schneier article does not disclose any sort of card initialization method; and

b. The Chen patent describes a card initialization method in which secret values are simply "stored" on a card (*i.e.*, transferred from processor to card) in a physically secured location.

Neither the Schneier article nor the Chen patent addresses the problem addressed by the present invention, namely securing card *initialization* in a way that does not involve any exchange of any part of the secret value. Neither Schneier nor Chen suggests card initialization in which no part of the secret value is exchanged in any form.

While Schneier might teach key generation based on stored secret values without actual public exchange of the secret values, *it does not disclose how the secret values were stored in the first place.* On the other hand, col. 4, lines 23-26 of the Chen patent simply describes the initialization key exchange as a key "**storage**" step. This clearly does not suggest parallel generation of keys in the manner claimed Instead of disclosing protection of keys during initialization, Chen discloses protecting the keys post-initialization, during transfer (*i.e.*, shipping) of the card to a customer, but only by a "**non-secret**" code (col. 4, lines 27-32). Again, this does not suggest parallel generation of keys, but rather suggests that Chen is not concerned with exchange security at all during initialization, since not even a non-secret key-protecting code is disclosed.

Because neither the Schneier article nor the Chen patent discloses or suggests the claimed chipcard ***initialization*** method in which only parts of values that are used to generate secret values are exchanged, it is respectfully submitted that the Schneier article and the Chen patent, whether considered individually or in any reasonable combination, could not possible have suggested the claimed invention, and withdrawal of the rejection of claims 1, 3-5, and 7 under 35 USC §103(a) is respectfully requested.

2. Rejection of Claim 2 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier), "Cryptographic Identification Methods..." (Konigs), "Handbook of Applied Cryptography" (Menezes), and U.S. Patent No. 5,602,918 (Chen)

This rejection is respectfully traversed on the grounds that the Konigs and Menezes articles, like the Schneier article and the Chen patent, fails to disclose or suggest a chipcard **initialization** step in which secret initial values are generated both at the card and at the processing station in the manner claimed, by exchange of values used to generate the secret values without actual exchange of any part of the secret initial values.

Instead, as mentioned in the previous response, the Konigs article discloses a method of establishing cryptographic data connections using chipcards without containing any suggestion as to how the chipcards used for the cryptographic data connections are initialized for use in the

cryptographic connections, while the Menezes publication merely teaches the use of sequence numbers to identify entities in key establishment protocols, and does not teach any specific initialization method of the type claimed. As a result, withdrawal of the rejection of claim 2 under 35 USC §103(a) is respectfully requested

3. Rejection of Claim 6 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 5,452,358 (Normile)

This rejection is respectfully traversed on the grounds that the Normile patent, like the the Schneier article and the Chen patent, fails to disclose or suggest a chipcard **initialization** step in which secret initial values are generated both at the card and at the processing station in the manner claimed, by exchange of values used to generate the secret values without actual exchange of any part of the secret initial values.

Instead, the Normile patent merely discloses public key encryption of a plaintext message. The public key of a private-public key pair can by definition be exchanged in public, and therefore there is no need to use parallel key generation. The private key, on the other hand, is maintained by only one party, and again there is no need for the claimed type of card initialization, which is useful for shared-secret key initialization but not for public-private key pair generation.

Because the Normile patent basically has nothing to do with the claimed invention, withdrawal of the rejection of claim 8 under 35 USC §103(a) in view of the Schneier article and the Chen and Normile patents is respectfully requested.

4. Rejection of Claim 8 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 6,038,551 (Barlow)

This rejection is respectfully traversed on the grounds that neither the Schneier article nor the Chen patent, whether considered individually or in any reasonable combination, discloses or suggests a chipcard **initialization** step that does not involve exchange of any part of secret values generated during the initialization.

Instead, the Barlow patent teaches a system that not only exchanges secret keys, but does so by means of public key encryption of the exchanged secret keys. Barlow makes no attempt to only exchange parts of secret values, but rather simply encrypts all of the values before exchange (col. 3, lines 1-13). This public key method of Barlow is not suitable for chipcard initialization of the type claimed, and Barlow does not even remotely suggest a method of generating an initialization value without exchanging the values. To the contrary, whereas the claimed invention is capable of generating initial values for each chipcard manufactured in a relatively simple and yet secure manner, Barlow teaches the difficulty of providing millions of different devices with individual keys, and instead suggests providing them all with a common *public* key. This essentially ***teaches away*** from the claimed invention.

Consequently, withdrawal of the rejection of claim 8 under 35 USC §103(a) in view of the Schneier article and the Chen and Barlow patents is respectfully requested.

5. Rejection of Claim 9 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen), 6,038,551 (Barlow), and 5,224,163 (Gasser)

This rejection is again respectfully traversed on the grounds that the Gasser patent, like the Chen and Barlow patents, fails to disclose a card **initialization** step in which transfer of data to the card is facilitated by a "secret value" exchange that only involves transfer of "parts" of the respective secret values, and that does not require transformation of the secret values.

Instead, the Gasser patent disclose generation of "session public/private encryption key pairs." The session public/private key pairs are generated, as is common in such session key generating schemes, by mutual exchange and processing of secret values, but there is no disclosure in the Gasser patent that the secret values used in the public/private session key generating process may be transferred to the chipcard by a secret value generated in the manner claimed, using parts of two picnics in the manner claimed.

Accordingly, withdrawal of the rejection of claim 9 under 35 USC §103(a) in view of the Schneier article and the Chen, Barlow, and Gasser patents is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: September 8, 2004

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500